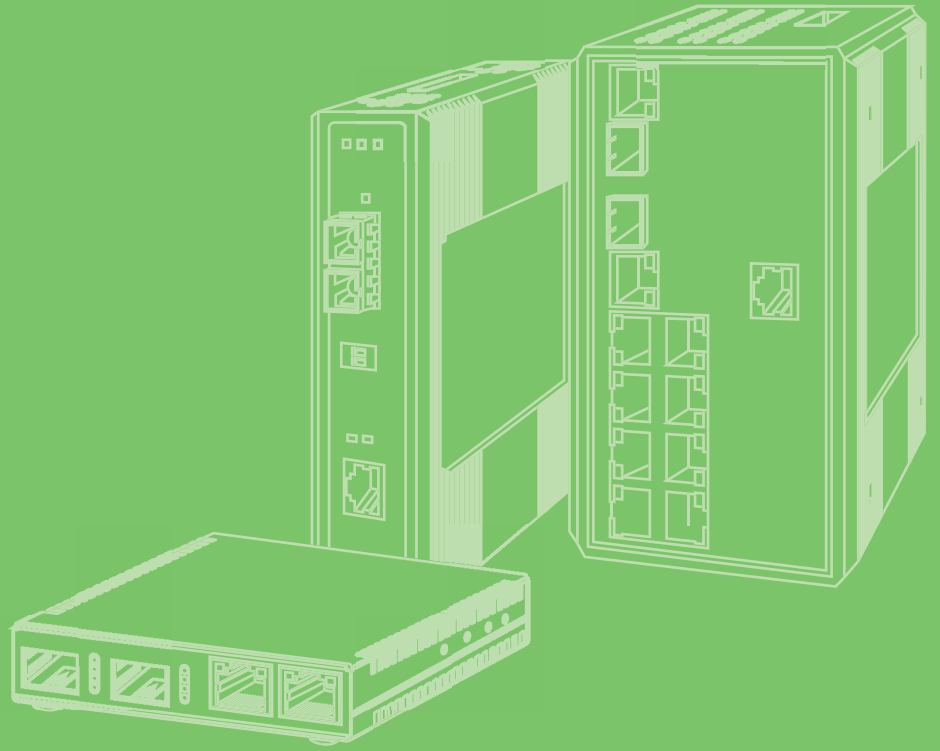


User Manual



SNMP Management Module (IMC-710-A)

ADVANTECH

Enabling an Intelligent Planet

Copyright

The documentation and the software included with this product are copyrighted 2021 by Advantech Co., Ltd. All rights are reserved. Advantech Co., Ltd. reserves the right to make improvements in the products described in this manual at any time without notice. No part of this manual may be reproduced, copied, translated or transmitted in any form or by any means without the prior written permission of Advantech Co., Ltd. Information provided in this manual is intended to be accurate and reliable. However, Advantech Co., Ltd. assumes no responsibility for its use, nor for any infringements of the rights of third parties, which may result from its use.

Acknowledgements

Intel and Pentium are trademarks of Intel Corporation.

Microsoft Windows and MS-DOS are registered trademarks of Microsoft Corp.

All other product names or trademarks are properties of their respective owners.

Product Warranty (5 years)

Advantech warrants to you, the original purchaser, that each of its products will be free from defects in materials and workmanship for five years from the date of purchase.

This warranty does not apply to any products which have been repaired or altered by persons other than repair personnel authorized by Advantech, or which have been subject to misuse, abuse, accident or improper installation. Advantech assumes no liability under the terms of this warranty as a consequence of such events.

Because of Advantech's high quality-control standards and rigorous testing, most of our customers never need to use our repair service. If an Advantech product is defective, it will be repaired or replaced at no charge during the warranty period. For out-of-warranty repairs, you will be billed according to the cost of replacement materials, service time and freight. Please consult your dealer for more details.

If you think you have a defective product, follow these steps:

1. Collect all the information about the problem encountered. (For example, CPU speed, Advantech products used, other hardware and software used, etc.) Note anything abnormal and list any on screen messages you get when the problem occurs.
2. Call your dealer and describe the problem. Please have your manual, product, and any helpful information readily available.
3. If your product is diagnosed as defective, obtain an RMA (return merchandise authorization) number from your dealer. This allows us to process your return more quickly.
4. Carefully pack the defective product, a fully-completed Repair and Replacement Order Card and a photocopy proof of purchase date (such as your sales receipt) in a shippable container. A product returned without proof of the purchase date is not eligible for warranty service.
5. Write the RMA number visibly on the outside of the package and ship it prepaid to your dealer.

Regulatory, Standards, Compliances

CE

This product has passed the CE test for environmental specifications. Test conditions for passing included the equipment being operated within an industrial enclosure. In order to protect the product from being damaged by ESD (Electrostatic Discharge) and EMI leakage, we strongly recommend the use of CE-compliant industrial enclosure products.

FCC Class A

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Technical Support and Assistance

1. Visit the Advantech web site at www.advantech.com/support where you can find the latest information about the product.
2. Contact your distributor, sales representative, or Advantech's customer service center for technical support if you need additional assistance. Please have the following information ready before you call:
 - Product name and serial number
 - Description of your peripheral attachments
 - Description of your software (operating system, version, application software, etc.)
 - A complete description of the problem
 - The exact wording of any error messages

Warnings, Cautions and Notes

Warning! *Important safety instructions save these instructions - this manual contains important safety instructions.*



Caution! *For use in a controlled environment. Refer to manual for environmental conditions.*



Note! *Notes provide optional additional information.*



Document Feedback

To assist us in making improvements to this manual, we would welcome comments and constructive criticism. Please send all such - in writing to:
ICG.Support@advantech.com

Statements, Precautions, Guidelines, Regulatory

FCC Radio Frequency Interference Statement

This equipment has been tested and found to comply with the limits for a Class A computing device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which the user will be required to correct the interference at his own expense.

Any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the equipment.

The use of non-shielded I/O cables may not guarantee compliance with FCC RFI limits. This digital apparatus does not exceed the Class A limits for radio noise emission from digital apparatus set out in the Radio Interference Regulation of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de classe A prescrites dans le Règlement sur le brouillage radioélectrique publié par le ministère des Communications du Canada.

Electrostatic Discharge (ESD) Precautions

Electrostatic discharge (ESD) can cause damage to any product, add-in modules or stand alone units, containing electronic components. Always observe the following precautions when installing or handling these kinds of products.

1. Do not remove unit from its protective packaging until ready to install.
2. Wear an ESD wrist grounding strap before handling any module or component. If the wrist strap is not available, maintain grounded contact with the system unit throughout any procedure requiring ESD protection.
3. Hold units by the edges; do not touch the electronic components or gold connectors.
4. After removal, always place boards on a grounded, static-free surface, ESD pad or in a proper ESD bag. Do not slide the modules or stand-alone units over any surface.

Warning! *Integrated circuits and fiber optic components are extremely susceptible to electrostatic discharge damage. Do not handle these components directly unless you are a qualified service technician and use tools and techniques that conform to accepted industry practices.*



Fiber Optic Cleaning Guidelines

Fiber Optic transmitters and receivers are extremely susceptible to contamination by particles of dirt or dust, which can obstruct the optic path and cause performance degradation. Good system performance requires clean optics and connector ferrules.

1. Use fiber patch cords (or connectors, if you terminate your own fiber) only from a reputable supplier; low-quality components can cause many hard-to-diagnose problems in an installation.

2. Dust caps are installed at the factory to ensure factory-clean optical devices. These protective caps should not be removed until the moment of connecting the fiber cable to the device. Should it be necessary to disconnect the fiber device, reinstall the protective dust caps.
3. Store spare caps in a dust-free environment such as a sealed plastic bag or box so that, when reinstalled, they do not introduce any contamination to the optics.
4. If you suspect that the optics have been contaminated, alternate between blasting with clean, dry, compressed air and flushing with methanol to remove particles of dirt.

Regulatory, Standards, Compliances

UL/CUL: Listed to Safety of Information Technology Equipment, including Electrical Business Equipment.

CE: The products described herein comply with the Council Directive on Electromagnetic Compatibility (2004/108/EC) and the Council Directive on Electrical Equipment Designed for use within Certain Voltage Limits (2006/95/EC). Conforms to UL Std. 60950-1; Certified to CSA Std. C22.2 No. 60950-1



Class 1 Laser product, Luokan 1 Laserlaite,
Laser Klasse 1, Appareil A'Lasers de Classe 1

European Directive 2002/96/EC (WEEE) requires that any equipment that bears this symbol on product or packaging must not be disposed of with unsorted municipal waste. This symbol indicates that the equipment should be disposed of separately from regular household waste. It is the consumer's responsibility to dispose of this and all equipment so marked through designated collection facilities appointed by government or local authorities. Following these steps through proper disposal and recycling will help prevent potential negative consequences to the environment and human health. For more detailed information about proper disposal, please contact local authorities, waste disposal services, or the point of purchase for this equipment.



RoHS

Copyright © 2021 Advantech. All rights reserved. The information in this document is subject to change without notice. Advantech assumes no responsibility for any errors that may appear in this document. SNMP Management Module is a trademark of Advantech. Other brands or product names may be trademarks and are the property of their respective companies.

Contents

Chapter 1	Product Overview	1
1.1	SNMP Management Module	2
1.2	Specifications	2
1.3	Hardware Views	3
1.3.1	Front View	3
1.3.2	System LED Panels	3
1.3.3	Installation Guidelines	3
1.3.4	Configuration	4
1.3.5	Using SNMP Write Lock Switch	4
Chapter 2	Web-HTTP Function	5
2.1	Web-HTTP	6
2.2	Serial Port Configuration	6
2.3	Using Telnet	6
2.4	Using DHCP	7
2.4.1	DHCP Disable (Static IP Addressing)	7
2.4.2	DHCP Enable (Dynamic IP Addressing)	7
2.5	Main Serial/Telnet Configuration Screen	7
Chapter 3	iView² Software Installation	10
3.1	Overview	11
3.2	Using iView ²	11
3.2.1	System Requirements	11
3.2.2	Other NMS Applications	11
3.3	iView ² (Webserver Version)	12
3.4	UMA (Unified Management Agent)	12
3.5	Easy Upgrades with the Unified Management Agent (UMA)	12
3.6	iView Passwords	12

List of Figures

Figure 1.1	Front View	3
Figure 1.2	System LED	3

Chapter 1

Product Overview

1.1 SNMP Management Module

The SNMP Management Module includes two twisted-pair ports: one for management, and one reserved for future use. The SNMP Management Module also features a DB-9 serial port. Both twisted-pair ports support the AutoCross feature that automatically selects between a crossover workstation or straight-through, depending on the connected device.

An iMediaChassis series with an installed Management Module connects to the LAN via an external 10/100 twisted-pair connection. Connect the chassis to the network by plugging one end of a CAT-5 twisted-pair cable into the port labeled MGMT on the Management Module. Plug the other end of the cable into a device (e.g., switch, etc.) in the existing Ethernet network.

Note! Some options require items that are sold separately.



1.2 Specifications

Specifications	Description	
Environmental*	Operating Temperature	0 to +50°C (+32 to +122°F)
	Storage Temperature	-6 to +71°C (+21 to +160°F)
	Operating Humidity	5 ~ 95°C (-41 ~ 203°F), non-condensing
Power	Power Consumption	600 mA @ 5V (typical)

*Intended for indoor and outdoor use.

1.3 Hardware Views

1.3.1 Front View

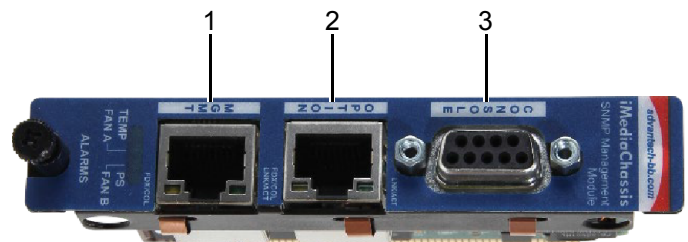


Figure 1.1 Front View

No.	Item	Description
1.	MGMT	RJ45 port for remote management.
2.	Option	ETH: 10/100BaseT(X) port
3.	Console	Console cable port to COM port (DB9 male) on computer to RS232 managed switch (RJ45 female).

1.3.2 System LED Panels

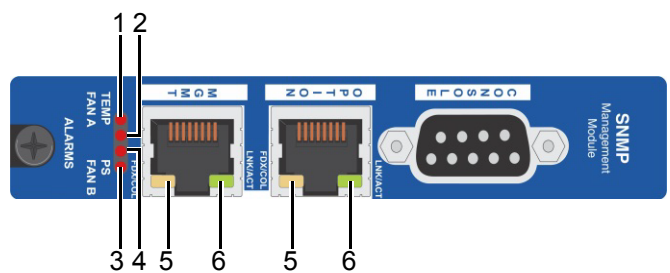


Figure 1.2 System LED

No.	Item	Description
1.	Temp	Glows yellow when temperature of unit surpasses a user-defined level; configurable through iView ² .
2.	Fan A	Refer to specific iMediaChassis series manuals for details.
3.	Fan B	Refer to specific iMediaChassis series manuals for details.
4.	PS	Glows amber when one power supply malfunctions.
5.	Link	Glows green when link is established on port.
6.	Activity	Glows green when data activity occurs.

1.3.3 Installation Guidelines

In order to manage an iMediaChassis series, available in 20, 6, or 3 slots, install the SNMP Management Module. Slide the SNMP Management Module into the first slot, on the far left of the chassis, using the card guides, and secure the module to the chassis by tightening the captive screw. This slot is ONLY for the Management Module; do not install application modules, such as media conversion and mode conversion modules, in this slot.

1.3.4 Configuration


Once connected to a network, assign the SNMP Management Module IP configuration information (e.g., IP address, subnet mask, etc.). There are four ways to do this:

- Using the Webserver version.
- Using the Management Module's serial port.
- Using DHCP (Dynamic Host Control Protocol); DHCP must be enabled through serial configuration or Telnet, via Web-HTTP.
- Telnet (Default IP=10.10.10.10; subnet mask 255.0.0.0)

In addition to assigning an IP address and subnet mask, the SNMP Management Module allows creation of community strings, assigning access rights, configuration of traps and more. After assigning an IP address, use iView² or another SNMP compatible Network Management System (NMS) to remotely configure, monitor and manage the modules installed.

1.3.5 Using SNMP Write Lock Switch

1. Ensure the SNMP Write Lock switch is set to **NORMAL**.
2. After configuring all application module settings via SNMP, use the Web-HTTP to make a backup copy of the SNMP management board's configuration.
3. If the SNMP Management Module needs to be replaced, set the SNMP Write Lock switch to **LOCKED**.
4. Remove the old SNMP module and replace with another SNMP module.
5. Connect to this SNMP module via Web-HTTP. Select **Tools->Upgrade Manager** on menu.
6. Select **HTTP** on Upgrade Method, and select **Startup configuration** on Upgrade type.
7. Find path of configuration file on Browse file, and click **Upgrade** button to upgrade configuration file.
8. Select **Tools->Reboot Device** on menu, and click Reboot button to reboot SNMP management.
9. After rebooting, set the SNMP Write Lock switch back to **NORMAL**. Previously made settings to the application modules will be active.

Note!  When removing an SNMP card with the SNMP Write Lock enabled (set to **LOCKED**), current application modules settings will not be changed. Never power-cycle the chassis while the SNMP Write Lock is enabled. Doing so will revert the SNMP card back to its original factory settings. (iView² should only be accessed with the SNMP Write Lock disabled.)

In the Write Lock Position, a field technician can test installation and removal of modules without generating Traps, such as Link Up, Link Down).

Chapter 2

Web-HTTP Function

2.1 Web-HTTP

Web-HTTP can let users quickly and easily complete the first stages of SNMP configuration for SNMP-manageable devices. Web-HTTP can set the IP address, subnet mask and default gateway as well as define the community strings and SNMP traps.

The Web-HTTP can be used to upload new versions of the system software and new MIB information. It also offers diagnostic capabilities for faster resolution of technical support issues. The default user ID for both Web-HTTP and Telnet is:

User: admin / Password: admin

The two levels of Telnet account access are:

- User: Can only see status, change password and reboot.
- Administrator: Can perform all functions and add/delete accounts and perform the command reset.

A Username and Password can be added in the User Account of Tools, or the Accounts command within Telnet or the Serial Configuration. Admin/admin should not be deleted until new usernames/passwords are tested. Refer to the Password section of this manual for additional information.

2.2 Serial Port Configuration

SNMP Management Modules used with the iMediaChassis series feature a serial port that includes a DB-9 serial connector. To connect an iMediaChassis series to a terminal/computer, use a straight-through (pin-to-pin) cable. If the computer/terminal's port is not compatible with a DB-9 COM port, use the pin connection chart for reference in making a cable.) Make sure the cable length is less than 15.24 meters (50 ft). Plug one end of the cable into the DB-9 connector and the other into the appropriate port on the computer/terminal.

Set the computer/terminal for VT-100 emulation. The serial port on the computer/terminal should be set for: 38.4K baud, 8 data bits, 1 stop bit, no parity, no flow control. The F2 key functions as a Delete key on VT-100 emulators.

Serial Adapter Pin Connection

RJ-45 Pin #	DB-9 Pin #	Function
5	2	Transmit (OUT)
7	3	Receive (IN)
8	5	Ground
1-4, 6	1, 4, 6-9	Reserved

2.3 Using Telnet

The iMediaChassis series supports Telnet for remote configuration. All configurations that can be performed via the serial port can also be performed using Telnet (except serial passwords). Use only one Telnet session at a time.

2.4 Using DHCP

2.4.1 DHCP Disable (Static IP Addressing)

DHCP is disabled in the default configuration. Initially, modules are assigned a Static default IP Address of 10.10.10.10. Changes to the Static IP Address can be added manually through Web-HTTP, an RS-232 Serial session, or Telnet. The changes will be initiated following reboot of the module.

2.4.2 DHCP Enable (Dynamic IP Addressing)

If a DHCP server is present on the network and DHCP is enabled, the DHCP client will initiate a dialog with the server during the boot up sequence. The server will then issue an IP address to the management card. Once the new IP address is received.

Refer to the About Serial Port Configuration for more information about Enabling/Disabling DHCP. When there is no DHCP server on the network, use serial configuration to manually set the IP addresses.

When DHCP is enabled, the IP address (default 10.10.10.10 or user configured) is saved. When DHCP is disabled, the saved IP address will be reinstated and the device will reboot.

DHCP servers give out lease times: devices renew their leases based on the administrator-specified time. If a device cannot renew its lease, and the lease expires, the device will be given the IP address 10.10.10.10.

2.5 Main Serial/Telnet Configuration Screen

After launching a serial session using a CLI (Command Line Interface) or a TELNET session, an initial self-test is performed and the main screen will display the following message: "Welcome to SNMP Management Module" and ready to accept user account/password.

2.5.0.1 Assigning IP Information

To modify the saved parameter values (i.e., assign IP address and subnet mask), key command `configure` to enter configure mode. Key command `ip address X.X.X.X mask X.X.X.X` to set the IP address and subnet mask for the connected device, and pressing Enter. (Key this command `ip address X.X.X.X.` to change IP address only)

When finished, key "exit" to leave configure mode and key command: "show ip". It will display now ip setting information.

2.5.0.2 Creating Community Strings for SNMP

The purpose of community strings is to add a level of security to a network. The default community string is named "public" and has read/write access. Do not delete the community string "public" until the new community string has been tested. Add necessary custom community strings such as one with read/only access (for general use), the other with read/write access (for the administrator).

To create a new community string, key in **configure** to enter configuration mode, key in **snmp community XXX rw** to add the name of the new community (up to 20 characters, no spaces) and community string's access rights, and press Enter. The following is the community string's access rights:

ro = read-only access

rw = read/write access

When finished, Key in **exit** to leave configuration mode, key in **show snmp** and press enter to display community information.

2.5.0.3 Deleting Community Strings

To delete specific community strings, key in **configure** to enter configuration mode. Key in **no snmp community XXXX** and press enter to delete.

2.5.0.4 Assigning Trap Destinations

A manageable device sends traps when certain events take place.

Key in **configure** to enter configuration mode, key in **snmp host x.x.x.x version 2c xxxx traps** (X.X.X.X is Ip address, xxxx is community name) and press enter to create trap destination. Key in **(no) snmp trap xxx** (xxx is trap type) and press enter to disable/enable trap type. This is following trap types: **auth, cold-start, linkUpDown, port-security and warm-start**.

To display trap destination, key in **show snmp** and press enter. To display activated or deactivated traps, key in **show snmp trap** and press enter.

2.5.0.5 Removing Trap Destinations

To remove specific trap destinations, key in **configure** to enter configuration mode, and key in **no snmp host x.x.x.x traps** (x.x.x.x is Ip address) and press enter to delete.

2.5.0.6 Enabling/Disabling DHCP

To Enable/Disable DHCP, Key in **configure** to enter configuration mode, and key in **(no) ip dhcp** and press enter to enable/disable DHCP.

2.5.0.7 Ending a Session

When ending a session, key in **exit** and press enter before disconnecting the cable in order to stop the device from continuing to send feedback status through to the serial port. If a session is not ended properly, the Telnet session cannot be launched.

2.5.0.8 Device-Specific Options— Downloading Files

With the iMediaChassis series, configuration file can be downloaded from a central server via a TFTP protocol. Initiate this download via serial configuration or Telnet session. Make sure the IP Address and the name of the file being downloaded are correct in the Current Values section of the Main Configuration screen.

To download a file, key in **copy startup-config tftp://x.x.x.x** (x.x.x.x is TFTP server IP) and press enter to download configuration file.

Chapter 3

iView² Software
Installation

3.1 Overview

All the options available through the Serial/Telnet session and more are available when using the software GUI of iView². The GUI is offered as a Webserver version; both can be downloaded from the Advantech website.

Note! *After January 2017, any new managed products will not be supported in the Desktop version.*



3.2 Using iView²

iView² is a network management application for Advantech intelligent networking devices. Graphic User Interface (GUI) gives network managers the ability to monitor and control products from a variety of platforms. The software is a free download, and available as a Webserver version.

3.2.1 System Requirements

To run iView², the management PC must be equipped with the following:

- 29 MB free disk space, 64 MB RAM.
- Windows NT 4.0 Service Pack 5, 2000 Professional, XP Professional.
- Microsoft SNMP Services Installed.
- Microsoft IE 4.0 or Higher.

iView² is a network management application for Advantech intelligent networking devices. It features a GUI that provides network managers the ability to monitor and control Advantech products. The application is available as a free download from the website.

iView² Webserver version requires the following:

- MySQL ver 5.1 or higher
- Apache/TomCat 6 or greater
- JAVA ver 1.7 or greater

Browsers required:

- MS Internet Explorer ver 10 or greater
- Mozilla Firefox ver 15.0 or greater
- Google Chrome ver 35 or greater

3.2.2 Other NMS Applications

If using an application other than iView² for management, integrate the SNMP MIBs into the vendor's NMS application. The MIBs are located in the MIB folder, a subdirectory of iView². If using the Webserver version of iView², on your PC's hard drive, go to Program

[Files\Apache Software Foundation\Tomcat_6_0\webapps\iView3\MIBS](#).

Note! *Be advised that unless you have an actual managed product connected to the network, that iView² identifies, you will not be able to locate the MIBs files.*



Refer to your application's documentation for information on how MIB files are integrated when not using iView. MIBs II are based on standard RFC 1213.

3.3 iView² (Webserver Version)

iView² is also available as a Webserver version. This is a browser-based software, which can be downloaded from the Advantech website. It offers more features than the Desktop version, such as supporting hundreds of users and particular Advantech manageable fiber devices. It still offers MIBs II and levels of security.

Refer to the “*Getting Started*” and “*Installation Instructions*” documents that are included with the Webserver download in the zip file, posted on the website.

3.4 UMA (Unified Management Agent)

Centralized management makes practical sense for networks of all sizes, especially service provider networks that must monitor and upgrade large quantities of devices. The Unified Management Agent (UMA) allows operators to manage all modules with Flash PROM (FiberLinX-II series) installed in an Advantech iMediaChassis series, with a single IP address from a central location. In addition, UMA allows users to centrally manage and administer firmware upgrades over multiple devices.

For example, install 20 iMcV-FiberLinX-II devices in a 20-slot iMediaChassis at the Central Office (CO) then connect each to a remote iMcV-FiberLinX-II unit installed at the customer's premise (CPE); UMA will then allow users to manage all devices (including the chassis at the CO) via a single IP address. Users may still assign IP addresses to each iMcV-FiberLinX-II and manage them independently when the SNMP Management Module within the iMediaChassis is omitted.

When an SNMP request for an iMcV-FiberLinX-II comes in, the SNMP Management Module in the iMediaChassis series passes the request to the SNMP agent in the specific module. The SNMP agent in the iMcV-FiberLinX-II provides the relevant management information, which is then routed via the SNMP Management Module and supplied to the client GUI (iView², version 1.8 or higher), as well as the serial port and Telnet.

3.5 Easy Upgrades with the Unified Management Agent (UMA)

- Upgrade one or multiple Host (CO) or Remote (CPE) devices with just a few mouse clicks. Refer to the iMcV-FiberLinX-II, iMcV-GigaFiberLinX, and IE-Mini FiberLinX-II series manuals for complete information.
- All devices in chassis are fully functional while upgrades are in process.
- Manage up to 41 devices with a single IP address.
- Only one Ethernet port is required, reducing the number of ports used on a network switch.

3.6 iView Passwords

Passwords are a way to make the management of network devices secure. If password accesses are lost, contact Advantech Technical Support.



Enabling an Intelligent Planet

www.advantech.com

Please verify specifications before quoting. This guide is intended for reference purposes only.

All product specifications are subject to change without notice.

No part of this publication may be reproduced in any form or by any means, electronic, photocopying, recording or otherwise, without prior written permission of the publisher.

All brand and product names are trademarks or registered trademarks of their respective companies.

© Advantech Co., Ltd. 2021